

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A) 平2-156357

⑬ Int. Cl.<sup>5</sup>

G 06 F 12/14  
11/30

識別記号

3 1 0 A  
3 0 5 H

庁内整理番号

7737-5B  
7343-5B

⑭ 公開 平成2年(1990)6月15日

審査請求 未請求 請求項の数 1 (全7頁)

⑮ 発明の名称 プログラム破壊防止方法

⑯ 特 願 昭63-310429

⑰ 出 願 昭63(1988)12月8日

⑱ 発 明 者 勝 又 幸 宏 神奈川県川崎市中原区上小田中1015番地 富士通株式会社  
内

⑲ 出 願 人 富士通株式会社 神奈川県川崎市中原区上小田中1015番地

⑳ 代 理 人 弁理士 井 桁 貞一

明 細 書

1. 発明の名称

プログラム破壊防止方法

2. 特許請求の範囲

メモリ上に展開された制御プログラムの指示に基づき動作するプロセッサと、該制御プログラムを展開するメモリと、該メモリに対する該プロセッサのアクセスを検出して、該プロセッサに割込み信号を送出するアクセス検出手段とを備えた装置の処理において、

該アクセス検出手段が送出する割込み信号により、該プロセッサが該制御プログラムの処理ステップから分岐して実行する破壊検出用プログラムを用意しておき、

該アクセス検出手段が割込み信号を送出した時、該メモリに対しプロセッサが送出したアドレスを抽出した後(7)、

該プロセッサのメモリに対するアクセスが書き込みか否かを調べ(8)、

メモリに対する書き込みであれば、該メモリに予め格納された破壊検出用プログラムの参照領域が指定するアクセス可能領域と書き込み禁止領域とアクセス禁止領域とを参照して、該メモリに対するアクセス可能領域を抽出し(9)、

前記抽出したアドレスの指示するメモリ領域が該アクセス可能領域であるかを調べ(10)、

アクセス可能領域であれば、処理中であった制御プログラムのステップの処理の実行に戻り(11)、

書き込み禁止領域又はアクセス禁止領域であれば、オペレーティングシステムに処理中であった制御プログラムのステップ情報を通知して(12)、制御プログラムの処理を中断し(13)、

該プロセッサのメモリに対するアクセスが書き込みでなければ、該メモリに予め格納された破壊検出用プログラムの参照領域を参照して、該メモリに対するアクセス可能領域と書き込み禁止領域とを抽出し(14)、

前記抽出したアドレスの指示するメモリ領域が該アクセス可能領域又は書き込み禁止領域であるか

を調べ、

アクセス可能領域又は書き込み禁止領域であれば、処理中であった制御プログラムのステップの処理の実行に戻り、

アクセス禁止領域であれば、オペレーティングシステムに処理中であった制御プログラムのステップ情報を通知して、制御プログラムの処理を中断すること(03)を特徴とするプログラム破壊防止方法。

### 3. 発明の詳細な説明

#### (概要)

プロセッサがメモリをアクセスする際に、メモリ上の制御プログラムを破壊することを防止するプログラム破壊防止方法に関し、

制御プログラムの破壊防止と、プロセッサの誤処理の原因究明を容易とすることを目的とし、

プロセッサと、メモリと、プロセッサのメモリアクセスを検出して割込み信号を送出するアクセス検出手段を備えた装置において、アクセス検出

手段の割込み信号で、プロセッサが制御プログラム処理から分岐して実行する破壊検出用プログラムを用意し、アクセス検出手段が割込み信号を送出した時、プロセッサが送出したアドレスを抽出し、書き込み可否かを調べ、書き込みならばメモリの参照領域が指定するアクセス可能領域と書き込み禁止領域とアクセス禁止領域を参照し、抽出したアドレスの指示するメモリ領域がアクセス可能領域ならば、制御プログラムの処理に戻り、そうでなければ、OSに処理中のステップ情報を通知して、制御プログラムの処理を中断し、書き込みでなければ、メモリの参照領域を参照して、抽出したアドレスの指示するメモリ領域がアクセス可能領域又は書き込み禁止領域であれば、制御プログラムのステップの処理に戻り、アクセス禁止領域であれば、OSに処理中のステップ情報を通知して、制御プログラムの処理を中断する構成とする。

#### (産業上の利用分野)

本発明はメモリ上に展開された制御プログラム

を読出して動作するプロセッサにより制御される装置に係り、特に該プロセッサが該メモリをアクセスする際に、該メモリ上の制御プログラムの破壊を防止するプログラム破壊防止方法に関する。

近年、プロセッサ制御による装置の高性能化、多目的化に伴い、該プロセッサの動作を指示する制御プログラムの高信頼性が要求されているが、この制御プログラムは装置の初期設定時に、ディスク装置等の外部記憶装置から読出されてRAM上に展開され、プロセッサがこのRAMをアクセスして制御プログラムを読出している。

このため、RAM上に展開された制御プログラムは、プロセッサが該RAMを誤ってアクセスすると、破壊されることがある。この場合、制御プログラムの一部が破壊され、プロセッサがプログラムの予期せぬ動作や誤動作をおこして暴走することがある。

従って、プロセッサが誤ってRAMをアクセスした場合、直ちに処理を中断させ、プロセッサが暴走することを阻止して、制御プログラムの破壊

されることを防止すると共に、プロセッサの誤アクセスの原因究明を容易とする必要がある。

#### (従来の技術)

従来はRAMの内容が書換えられ、プロセッサの暴走等の不具合が発生した後に、RAMの内容をダンプさせ、制御プログラムやデータの内容を検査し、プロセッサの暴走原因を調べている。

#### (発明が解決しようとする課題)

上記の如く、従来はプロセッサの暴走等が発生した後に、その原因を調べているため、プロセッサの暴走により制御プログラムが連続して破壊されていることが多く、プロセッサがRAMを誤アクセスした時の制御プログラムの実行内容を調べることが、タイミング的に困難であり、このため、プロセッサの誤動作の原因究明に多くの時間を必要とするという問題がある。

本発明はこのような問題点に鑑み、プロセッサがRAMを誤アクセスした場合、直ちに処理を中

断させ、制御プログラムが連続して破壊されることを防止し、プロセッサの誤処理の原因究明を容易とすることを目的としている。

(課題を解決するための手段)

第1図は本発明の構成を示す処理の流れ図である。

第1図はメモリ上に展開された制御プログラムを読出して動作するプロセッサにより制御される装置のプロセッサの処理の流れを示し、7〜14は処理のステップである。

(作用)

メモリ上に展開された制御プログラムの指示に基づき動作するプロセッサと、該制御プログラムを展開するメモリと、該メモリに対する該プロセッサのアクセスを検出して、該プロセッサに割込み信号を送出するアクセス検出手段とを備えた装置のプロセッサはアクセス検出手段が割込み信号を送出すると、処理ステップ7でメモリに対しブ

において、オペレーティングシステム(以後OSと略す)に処理中であった制御プログラムのステップ情報を通知する。即ち、制御プログラムのどのステップまで処理したかを通知する。そして、処理ステップ13で制御プログラムの処理を中断する。

処理ステップ8でプロセッサが送出した命令が書込み命令でない場合、即ち、読出し命令であった場合は、処理ステップ14で、メモリに予め格納されている破壊検査用プログラムの参照領域を参照し、この参照領域が指定するアクセス可能領域と、書込み禁止領域と、アクセス禁止領域の中から、メモリに対するアクセス可能領域と書込み禁止領域を読出す。

そして、処理ステップ15において、処理ステップ7で抽出したアドレスが指示するメモリ領域が、処理ステップ14で読出したアクセス可能領域又は書込み禁止領域を指示していれば、処理ステップ11で、処理中であった制御プログラムのステップの処理の実行に戻る。

ロセッサが送出したアドレスを抽出する。

そして、処理ステップ8でプロセッサがメモリに対し書込み命令を送出したか調べる。

処理ステップ8で書込み命令が送出されていると、処理ステップ9において、メモリに予め格納されている破壊検査用プログラムの参照領域を参照し、この参照領域が指定するアクセス可能領域と、書込み禁止領域と、アクセス禁止領域の中から、メモリに対するアクセス可能領域を読出す。

そして、処理ステップ10において、処理ステップ7で抽出したアドレスが指示するメモリ領域が、処理ステップ9で読出したアクセス可能領域を指示していれば、処理ステップ11で、処理中であった制御プログラムのステップの処理の実行に戻る。

処理ステップ10において、処理ステップ7で抽出したアドレスが指示するメモリ領域が、処理ステップ9で読出したアクセス可能領域を指示していなければ、即ち、書込み禁止領域又はアクセス禁止領域を指示していれば、処理ステップ12

処理ステップ15において、処理ステップ7で抽出したアドレスが指示するメモリ領域が、処理ステップ14で読出したアクセス可能領域又は書込み禁止領域を指示していなければ、即ち、アクセス禁止領域を指示していれば、前記同様に、処理ステップ12と13を実行する。

以上により、プロセッサが送出したアドレスが誤っているか否かを検出し、誤っていれば直ちに制御プログラムの処理を中断し、処理中であった制御プログラムのステップ情報をOSに通知することが可能となる。

従って、制御プログラムを連続して破壊することを防止すると共に、プロセッサの誤処理の原因究明を容易とすることが出来る。

(実施例)

第2図は本発明の一実施例を示す回路のブロック図で、第3図は第2図の動作を説明するフローチャートで、第4図は制御プログラムの展開状態を説明する図で、第5図は破壊検出用プログラム

参照領域を説明する図である。

プロセッサ1は初期設定時に、ROM3にアドレスバスを経てアドレスを送出し、データバスを経て初期設定用のプログラムを読出して動作を開始する。そして、外部記憶装置4にアドレスを送出して、制御プログラムと、この制御プログラムを遂行するために必要なデータを読出す。

そして、制御バスを経てRAM5に書込み命令を送出し、アドレスバスを経てRAM5にアドレスを送出し、外部記憶装置4からデータバスを経て読出された制御プログラムとデータを、該アドレスに対応した領域に第4図に示す如く展開して書込ませる。

制御プログラムはRAM5上に展開される場合、複数のプログラムが共通に使用するデータを格納する共通データ領域と、各プログラムが専用使用するデータを格納するデータ領域、即ち、プログラムA用データ領域と、プログラムB用データ領域と、その他のプログラム用データ領域、及び各プログラムが夫々格納されている領域、即ち、

域に書込まれる。

第4図⑩に示す領域は、本発明の破壊検出用プログラムが参照する領域、即ち、破壊検出用プログラム参照領域である。

この破壊検出用プログラム参照領域の詳細は第5図に示す如くである。即ち、領域の欄に示す①～⑨は第4図の①～⑨に対応し、プログラムAの動作時には、RAM5の領域①は第4図①が示す如く、書込み禁止の領域であり、RAM5の領域②は第4図②に示す如く、アクセス可能な領域であり、RAM5の領域③は第4図③に示す如く、書込み禁止の領域であり、RAM5の領域④は第4図④に示す如く、アクセス可能な領域である。

そして、RAM5の領域⑤はプログラムB専用のデータ格納領域であるため、プログラムAにとってはアクセスしてはならないアクセス禁止の領域であり、同様にRAM5の領域⑥はアクセス禁止の領域であり、RAM5の領域⑦は第4図⑦に示す如く、書込み禁止の領域であり、RAM5の領域⑧は、プログラムBが格納されているため、

プログラムA格納領域と、プログラムB格納領域と、その他のプログラム格納領域とに分かれる。

又、共通データ領域に書込まれるデータの中には、書替えてはいけなないデータの如きデータがあり、このようなデータは第4図①に示す如く、書込み禁止領域に書込まれ、書替えても良いデータは第4図②に示す如く、アクセス可能領域、即ち、書込み／読出しが可能な領域に書込まれる。

同様にプログラムA用データ領域も、第4図③に示す如く、書替えてはいけなないデータは書込み禁止領域に書込まれ、書替えても良いデータは第4図④に示す如く、アクセス可能領域に書込まれる。

同様にプログラムB用データ領域も、第4図⑤に示す如く、書替えてはいけなないデータは書込み禁止領域に書込まれ、書替えても良いデータは第4図⑥に示す如く、アクセス可能領域に書込まれる。

又、第4図⑦⑧に示す如く、プログラムA及びB自身は書替えてはならないため、書込み禁止領

域プログラムAにとってはアクセス禁止の領域である。

又、RAM5の領域⑨は、破壊検出用プログラム専用の参照領域であるため、プログラムAにとってはアクセス禁止の領域となる。

同様にプログラムBが動作時には、RAM5の領域①と⑤と⑧が書込み禁止の領域であり、②と⑥がアクセス可能な領域であり、③と④と⑦と⑨がアクセス禁止の領域である。

又、プログラムA及びB以外の他プログラム動作時には、①が書込み禁止の領域で、②がアクセス可能な領域で、③～⑨はアクセス禁止の領域となる。

プロセッサ1はRAM5に制御プログラムが格納されると、制御バスを経てRAM5に読出し命令を送出し、アドレスバスを経てアドレスをRAM5に送出し、制御プログラムやデータをデータバスに読出させ、この制御プログラムの指示に従いデータを使用して処理を行う。

プロセッサ1は第3図⑩、⑪に示す如く、制御

プログラムの各ステップを順次実行し、ステップ⑩において、RAMアクセス命令が指示されていると、プロセッサ1は前記の如く、制御バスを経てRAM5に書き込み命令又は読出し命令を送出し、アドレスバスを経てアドレスを送出する。

アクセス検出回路6はアドレスバスを経て、プロセッサ1がRAM5にアドレスを送出したことを検出すると、データバスを経て割込み制御回路2に、RAM5がプロセッサ1にアクセスされたことを通知する。割込み制御回路2は、この通知を受信するとプロセッサ1に割込み信号を送出し、破壊検出用プログラムの実行を指示する。

プロセッサ1は内部メモリ等に格納してある破壊検出用プログラムを読出して、この破壊検出用プログラムの指示により動作し、制御プログラムの第3図⑩に示すステップから分岐して、破壊検出用プログラムの処理を実行するため、第3図⑪に示す如く、第3図⑩のステップで指示されたRAMアクセス命令からアドレスを抽出する。そして、第3図⑫に示す如く、RAMアクセス命令が

書き込み命令であるか否かを調べる。

RAMアクセス命令が書き込み命令であった場合、プロセッサ1は第3図⑬に示す如く、RAM5に展開した制御プログラムの第4図⑭に示す⑨の領域を参照する。即ち、第4図⑭の領域を参照し、アクセス可能領域を読出す。そして、第3図⑮に示す如く、⑫は⑨の領域指示かを調べる。即ち、第3図⑯で抽出したアドレスが、プログラムAが動作時であれば、第5図の領域②又は領域④を指示しているかを調べ、プログラムBが動作中であれば、第5図の領域②又は領域⑥を指示しているかを調べる。

第3図⑮で⑫は⑨の領域を指示していると判定された場合、第3図⑩のRAMアクセス命令は正常であると判定し、プロセッサ1は第3図⑮に示す如く、第3図⑩のステップで指示されたRAMアクセス命令を実行するが、⑫が⑨の領域を指示していないと判定された場合、第3図⑩のRAMアクセス命令は異常であると判定し、第3図⑯に示す如く、OSに実行中であった制御プログラム

のステップ情報を通知し、第3図⑰に示す如く、制御プログラムの処理を中断する。

即ち、制御プログラムのどのステップまで処理したか、OSに通知して動作を停止するため、書き込み禁止領域又はアクセス禁止領域のアドレスを誤って送出した原因調査を容易とすることが出来る。

第3図⑰のステップにおいて、RAMアクセス命令が書き込み命令ではなかった場合、プロセッサ1は読出し命令であると判定し、第3図⑱に示す如く、第4図⑱の領域を参照し、アクセス可能と書き込み禁止の領域を読出す。

そして、第3図⑲に示す如く、⑫は⑨の領域指示かを調べる。即ち、第3図⑲で抽出したアドレスが、プログラムAが動作時であれば、第5図の領域①、②、③、④、⑦のどれかを指示しているかを調べ、プログラムBが動作中であれば、第5図の領域①、②、⑤、⑥、⑧のどれかを指示しているかを調べる。

第3図⑲で⑫は⑨の領域を指示していると判定

された場合、プロセッサ1は第3図⑲に示す如く、第3図⑩のステップで指示されたRAMアクセス命令を実行するが、⑫は⑨の領域を指示していないと判定された場合、第3図⑲に示す如く、OSに実行中であった制御プログラムのステップ情報を通知し、第3図⑲に示す如く、制御プログラムの処理を中断する。

#### (発明の効果)

以上説明した如く、本発明はプロセッサがRAMを誤アクセスした場合、直ちに処理を中断させ、OSに制御プログラムの処理したステップ情報を通知させるため、制御プログラムが連続して破壊されることを防止し、プロセッサの誤処理の原因究明を容易とすることが出来る。

#### 4. 図面の簡単な説明

第1図は本発明の構成を示す処理の流れ図、

第2図は本発明の一実施例を示す回路のブロック図、

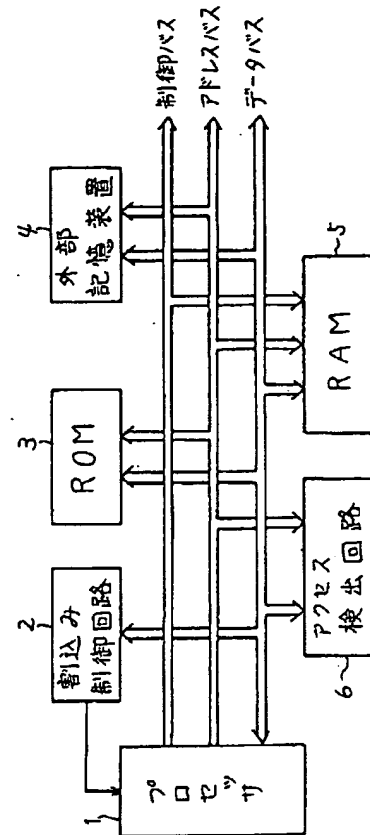
第3図は第2図の動作を説明するフローチャート、  
第4図は制御プログラムの展開状態を説明する図、  
第5図は破壊検出プログラム参照領域を説明する  
図である。

図において、

- 1 はプロセッサ、 2 は割込み制御回路、  
3 はROM、 4 は外部記憶装置、  
5 はRAM、 6 はアクセス検出回路、  
7~18 は処理ステップである。

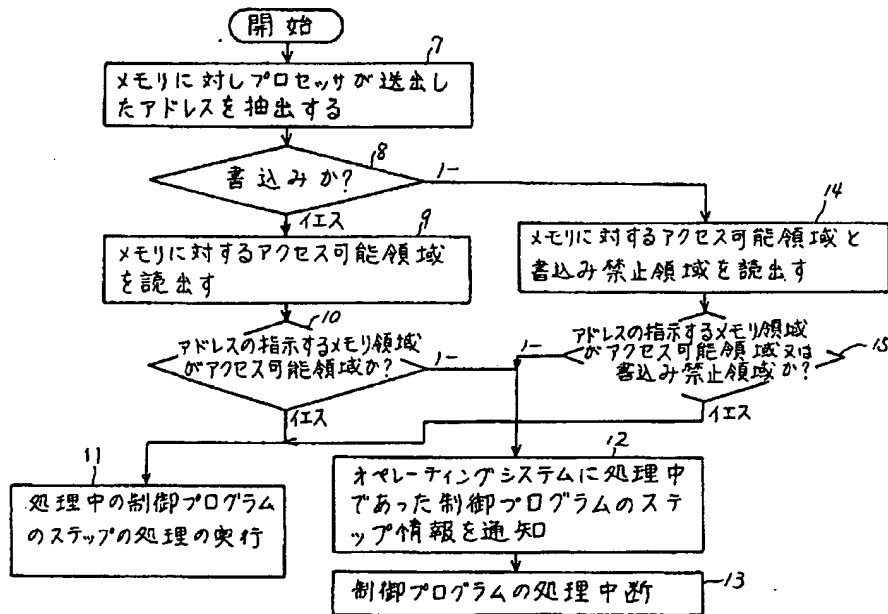
代理人弁理士

井桁貞一



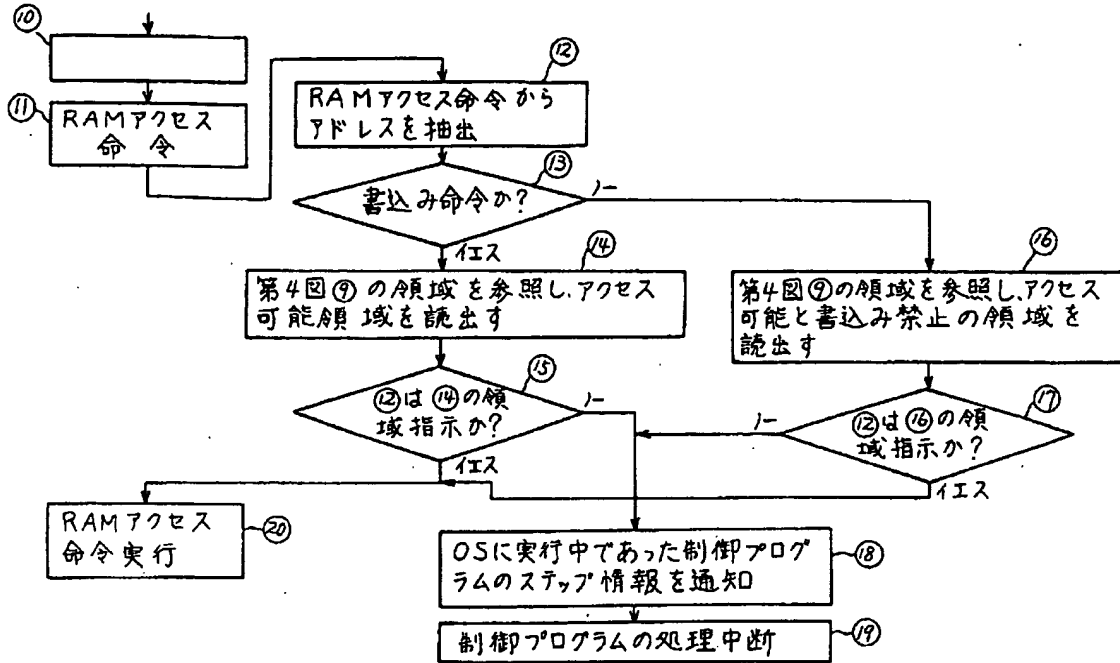
本発明の一実施例を示す回路のブロック図

第2図



本発明の構成を示す処理の流れ図

第1図



第2図の動作を説明するフローチャート

第 3 図

①	共通データ領域	(書き込み禁止領域)
②		(アクセス可能領域)
③	プログラムA用データ領域	(書き込み禁止領域)
④		(アクセス可能領域)
⑤	プログラムB用データ領域	(書き込み禁止領域)
⑥		(アクセス可能領域)
...		
⑦	プログラムA格納領域	(書き込み禁止領域)
⑧	プログラムB格納領域	(書き込み禁止領域)
...		
⑨	破壊検出用プログラム参照領域	(アクセス禁止領域)

制御プログラムの展開状態を説明する図

第 4 図

領域	プログラムA動作時	プログラムB動作時	他プログラム動作時
①	書き込み禁止	書き込み禁止	書き込み禁止
②	アクセス可能	アクセス可能	アクセス可能
③	書き込み禁止	アクセス禁止	アクセス禁止
④	アクセス可能	アクセス禁止	アクセス禁止
⑤	アクセス禁止	書き込み禁止	アクセス禁止
⑥	アクセス禁止	アクセス可能	アクセス禁止
⑦	書き込み禁止	アクセス禁止	アクセス禁止
⑧	アクセス禁止	書き込み禁止	アクセス禁止
⑨	アクセス禁止	アクセス禁止	アクセス禁止

破壊検出用プログラム参照領域を説明する図

第 5 図